Вестник Астраханского государственного технического университета.
Серия: Управление, вычислительная техника и информатика. 2025. № 1
Vestnik of Astrakhan State Technical University.
Series: Management, computer science and informatics. 2025. N. 1
ISSN 2072-9502 (Print), ISSN 2224-9761 (Online)

КОМПЬЮТЕРНОЕ ОБЕСПЕЧЕНИЕ И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

COMPUTER ENGINEERING AND SOFTWARE

Научная статья
УДК 004.056.5
https://doi.org/10.24143/2072-9502-2025-1-46-55
EDN EIWRKM

Анализ момента ближайшей атаки в объектах критической инфраструктуры при степенном изменении интенсивности атак во времени

Г. А. Попов, Н. В. Давидюк, К. Д. Кузовлев✉, Ш. Ш. Иксанов, А. С. Сафаралиев

Астраханский государственный технический университет,
Астрахань, Россия, k.kuzovlev@astu.org✉

Аннотация. На основе аппарата регенерирующих процессов проводится анализ модели, описывающей процесс злонамеренных атак на защищаемый объект критической информационной инфраструктуры (КИИ). Предполагается: интервалы между последовательными моментами подготовки и реализации злоумышленных атак независимы в совокупности. Эти интервалы применительно к каждому из источников атак достаточно велики, источники между собой не общаются. Вероятность успешной атаки от одного источника достаточно мала, поэтому моменты успешной атаки для каждого из источников атак достаточно далеко удалены друг от друга. Как следствие, событие, связанное с успешным для злоумышленника завершением атаки, представляет собой редкое событие. Однако ввиду того, что успешная атака на объект КИИ порождает большие потери и издержки, возникает необходимость изучения рассматриваемого процесса. Основной исследуемой характеристикой в рамках описанной модели является первый (ближайший) момент успешного совершения злоумышленной атаки. Данная характеристика относится к числу наиболее важных для процесса противодействия атакам. Числовые оценки параметров момента совершения первой успешной атаки позволят более адаптивно организовать процесс противодействия атакам, осуществив на наиболее опасных и уязвимых интервалах времени дополнительные меры по обеспечению информационной безопасности. Анализ этой характеристики выполнен в условиях наличия неоднородности поведения всего процесса противостояния атак и противодействия им. Предполагается, что интервалы между последовательными моментами атак и вероятности успешности атак во времени изменяются по степенному закону в среднем. Это предположение отражает процесс динамического изменения в источниках атак и в системе защиты объекта КИИ. Выведено асимптотическое соотношение для нормированной величины момента совершения первой атаки в условиях, когда интервалы между последовательными моментами совершения атак неограниченно растут, но при этом и число источников атак увеличивается так, что средняя доля успешных атак стремится к некоторому ненулевому пределу. Получены асимптотические выражения для среднего времени до ближайшей атаки.

Ключевые слова: информационная безопасность, объект критической инфраструктуры, первая успешная атака, неоднородный регенерирующий процесс, редкое событие, асимптотическое поведение, степенное изменение во времени

Для цитирования: *Попов Г. А., Давидюк Н. В., Кузовлев К. Д., Иксанов Ш. Ш., Сафаралиев А. С.* Анализ момента ближайшей атаки в объектах критической инфраструктуры при степенном изменении интенсивности атак во времени // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2025. № 1. С. 46–55. https://doi.org/10.24143/2072-9502-2025-1-46-55. EDN EIWRKM.

Original article

Analysis of the nearest attack moment in critical infrastructure objects with a gradual change in the intensity of attacks over time

G. A. Popov, N. V. Davidyuk, K. D. Kuzovlev✉, Sh. Sh. Iksanov, A. S. Safaraliev

Astrakhan State Technical University,
Astrakhan, Russia, k.kuzovlev@astu.org✉

Abstract. Based on the apparatus of regenerating processes, a model is analyzed that describes the process of malicious attacks on a protected object of critical information infrastructure (CII). It is assumed that the intervals between the successive moments of preparation and implementation of malicious attacks are completely independent. These intervals are quite large for each of the attack sources, and the sources do not communicate with each other. The probability of a successful attack from a single source is quite low, so the moments of a successful attack for each of the attack sources are far enough apart from each other. As a result, the event associated with the successful completion of the attack for the attacker is a rare event. However, due to the fact that a successful attack on a CII facility generates large losses and costs, it becomes necessary to study the process under consideration. The main characteristic under study within the framework of the described model is the first (nearest) moment of successful malicious attack. This characteristic is one of the most important for the process of countering attacks. Numerical estimates of the parameters of the moment of the first successful attack will make it possible to more adaptively organize the process of countering attacks by implementing additional information security measures at the most dangerous and vulnerable time intervals. The analysis of this characteristic was performed in the context of the heterogeneity of the behavior of the entire process of countering attacks and countering them. It is assumed that the intervals between successive moments of attacks and the probabilities of attack success vary over time according to a power law on average. This assumption reflects the process of dynamic change in the sources of attacks and in the protection system of the CII facility. An asymptotic relationship is derived for the normal value of the moment of the first attack in conditions when the intervals between successive moments of attacks grow indefinitely, but at the same time the number of attack sources increases so that the average proportion of successful attacks tends to a certain non-zero limit. Asymptotic expressions for the average time to the nearest attack are obtained.

Keywords: information security, critical infrastructure object, time of the nearest successful attack, non-homogeneous regenerative processes, rare events, asymptotic behavior, power-law variation over time

For citation: Popov G. A., Davidyuk N. V., Kuzovlev K. D., Iksanov Sh. Sh., Safaraliev A. S. Analysis of the nearest attack moment in critical infrastructure objects with a gradual change in the intensity of attacks over time. *Vestnik of Astrakhan State Technical University. Series: Management, computer science and informatics*. 2025;1:46-55. (In Russ.). https://doi.org/10.24143/2072-9502-2025-1-46-55. EDN EIWRKM.

Введение

В настоящее время объекты ключевой информационной инфраструктуры (КИИ) в России подвергаются интенсивным атакам на всех уровнях: физическом, информационном, военно-диверсионном и др., поэтому задача повышения их надежности и защищенности является актуальной. Ввиду высокой защищенности объектов КИИ вероятность совершения злонамеренной успешной атаки крайне мала, но возможный ущерб может быть очень большим, т. е. риски в сфере обеспечения информационной безопасности (ИБ) в результате достаточно значимы, поэтому целесообразно их оценить. Ключевой характеристикой, необходимой для оценки рисков, является совокупная вероятность успешности злонамеренной атаки. Именно эта характеристика и рассматривается в работе. Ввиду малой величины вероятностей и редкости успешных атак для изучения указанных вероятностей предлагается использовать аппарат редких регенерирующих процессов [1–3]. В данной работе рассматривается задача оценки вероятностей возможных атак на объекты КИИ во времени. Опишем рассматриваемую модель более детально.

Модель противоборства злоумышленным атакам

Процесс совершения атак на объект защиты достаточно адекватно описывается восстанавливаемыми системами с очень малой вероятностью происшествия некоторого редкого события. В рамках данной работы таковым является совершение успешной для злоумышленника атаки на объект защиты, примеры приведены в [1–3]. С точки зрения противодействия атакам на объект защиты наибольший интерес представляет ближайший, начиная с данного, момент успешной атаки злоумышленника. Знание этой характеристики позволит более адекватно и своевременно предпринимать меры по противодействию атаке. Применительно к введенной модели на основе регенерирующих процессов данная характеристика описывает момент первого наступления некоторого (редкого) события [2].

В настоящее время для однородных регенерирующих процессов успешно реализован подход, опирающийся на результат А. Д. Соловьева [3]. Однако применительно к процессам обеспечения ИБ условие однородности, как правило, не выполняется. Это связано, прежде всего, с тем, что злоумышленный источник активно, агрессивно ищет новые возможности для проникновения на объект защиты и к защищаемым ресурсам, постоянно совершенствуя и изменяя свои методы и приемы злоумышленного проникновения. Поэтому необходимо обобщить результаты работ по однородным процессам на случай неоднородных регенерирующих процессов. Подобный результат для случая неоднородных процессов был ранее получен в работе [4]. Указанный ниже результат уточняется для важного частного случая, когда характеристики процесса противодействия с течением времени изменяются достаточно регулярным (степенным) образом. Данное предположение вполне приемлемо для сферы ИБ, поскольку в этой сфере резкие революционные изменения в средствах атак и методах противодействия практически не происходят, идет непрерывное устойчивое развитие возможностей как атак, так и средств противодействия им.

Таким образом, работа посвящена получению асимптотической оценки для момента времени совершения первой успешной для злоумышленника атаки на информационные ресурсы объекта защиты, относящегося к объектам КИИ. Предлагаемое решение опирается на методы анализа неоднородных регенерирующих процессов. Работ по неоднородным регенерирующим процессам применительно к данной сфере в доступной литературе найти не удалось. По общей теории однородных регенерирующих процессов достаточно полный обзор приведен в [2]. Работ по использованию аппарата регенерирующих процессов в сфере ИБ найти не удалось, за исключением работ с участием одного из авторов [4–6]. В данной работе основной теоретический результат работы [4] доказывается для случая степенного изменения во времени основных характеристик модели. Представляет интерес работа [7], также отсылающая к исследованию описанной характеристики.

Формализация задачи и предварительные сведения

Для формализации описанной выше задачи приведем вначале ограничения и условия, которые обеспечивают определенную асимптотическую согласованность основных характеристик модели [4].

Пусть задан регенерирующий процесс $\kappa(t)$ с точками регенерации $t_0 = 0 < t_1 < t_2 < \ldots < t_n < \ldots$; положим $\xi_n = t_n - t_{n-1}$. Далее, на промежутке $[t_{n-1}, t_n)$ в некоторый момент $t_{n-1} + \eta_n$ $(0 \le \eta_n < \xi_n)$ возможно возникновение события A_n, представляющего собой успешную для злоумышленника завершившуюся атаку на информационные ресурсы объекта защиты. Предполагается, что событие A_n и промежуток времени η_n не зависят от значений процесса $\kappa(t)$ вне промежутка $[t_{n-1}, t_n)$. Через χ_k обозначим индикатор события A_k: $\chi(A_k\} = 1$, когда событие A_k происходит, и $\chi(A_k\} = 0$, если не происходит. Основной изучаемой характеристикой является момент τ_n первого после t_{n-1} происшествия одного из событий A_k $(k \ge n)$, т. е. успешной для злоумышленника реализации злонамеренной атаки, $\varsigma_n \overset{def}{=} \xi_n(1 - \chi_n) + \eta_n \chi_n$. Введем обозначения $(n \ge 1;\ z \ge 0)$:

$$\varphi_n(z) = M(e^{-z\xi_n});\ \overline{\varphi}(z) = 1 - \varphi_n(z);\ q_n = P\{\chi_n = 1\};$$

$$\varphi_n^-(z) = M(e^{-z\varsigma_n}\chi_n);\ \varphi_n^+(z) = M(e^{-z\varsigma_n}(1 - \chi_n));\ \pi_n(z) = \overline{\varphi}_n(z) + \varphi_n^-(z),$$

где M – знак математического ожидания. Отметим, что $\overline{\varphi_n}(0) = 0$ и $\varphi_n^-(0) = q_n$.

В работе изучается асимптотическое поведение момента τ_n в условиях, когда число источников атак растет, но сами атаки становятся более редкими. Указанное положение формализуется путем введения некоторого малого параметра, и чем меньше значение этого параметра, тем меньше значение уменьшения вероятностей редких событий. Таким образом, все перечисленные выше характеристики зависят также от некоторой переменной (параметра) $\gamma \in \Theta$: $q_n = q_n(\gamma)$, $\varphi_n^-(z) = \varphi_n^-(\gamma, z)$, $\pi_n(z) = \pi_n(\gamma, z)$, где Θ – множество допустимых значений переменной γ, представляющее собой интервал или дискретное множество на числовой оси, причем точка 0 есть предельная точка этого множества, поэтому запись «$\gamma \to 0$» ниже равносильна условию: $\gamma \to 0$ так, что $\gamma \in \Theta$.

Для формулировки и доказательства основных утверждений работы воспользуемся условиями на введенные характеристики, которые сформулированы в [4]. Для обеспечения асимптотической сходимости введенных регенерирующих процессов необходимо потребовать определенную регулярность поведения основных характеристик системы. Данное требование в работе охвачено условиями А и Д, приводимыми ниже.

А. Существуют нормирующие функции $g_n(\gamma)$ и $m(\gamma)$ $(n \geq 1, \gamma \in \Theta)$ такие, что $\lim\limits_{\gamma \to 0} m(\gamma) = \lim\limits_{\gamma \to 0} g_n(\gamma) = 0$, и для произвольного $n \geq 1, z > 0$ выполнено соотношение

$$\lim_{\gamma \to 0}\left\{\overline{\varphi}_n\left(m(\gamma)z\right)\left(g_n(\gamma)\right)^{-1}\right\} \cdot \omega_n(z);\ \omega_n(1) = 1. \tag{1}$$

Отметим, что функции $g_n(\gamma)$ описывают скорость стремления к нулю длительностей промежутков между последовательными моментами совершения атак.

Требование исчезающей редкости злоумышленных действий сформулировано в условии Б; количество точек регенерации на конечном промежутке и, соответственно, попыток злоумышленных действий согласованы в условии В. При этом рост числа интервалов и количества злоумышленных попыток также должны быть синхронизированы для обеспечения определенной регулярности поведения всей модели – условие Г.

Б. Справедливо соотношение $\lim\limits_{\gamma \to 0} \sup\limits_{n \geq 1} q_n(\gamma) = 0$.

Прежде чем описывать остальные условия, введем обозначения $n \leq 1, z > 0$:

$$S_1(n, \gamma) = \sum_{k=1}^{n} q_k(\gamma);\quad S_2(n, \gamma) = \sum_{k=1}^{n} g_k(\gamma).$$

С целью упрощения изложения материала ниже, наряду с обозначением $S_i(n, \gamma)$, используется также обозначение $S_i(n)$.

В. Для любых $\gamma > 0$ и целых $n > 0$ справедливы соотношения

$$S_i(n) = n^{\theta_i} L_i(n) \cdot G_i(\gamma)\ (1 + \alpha_i(n, \gamma)),\ i = \overline{1, 2}, \tag{2}$$

где $\theta_i \geq 0$, $L_i(x)$ $(x > 0)$ – медленно меняющаяся функция, $\lim\limits_{n \to \infty, \gamma \to 0} \alpha_i(n, \gamma) = 0$.

При этом справедливы соотношения [4]

$$\lim_{\gamma \to 0} G_i(\gamma) = 0,\ i = \overline{1, 2}. \tag{3}$$

Соотношение (2) и определяет степень регулярности изменения основных характеристик модели в схеме серий, в рамках которой доказывается основной результат. Соотношения (2) и (3) гарантируют существование функций $\lambda_1(\gamma)$ и $\lambda_2(\gamma)$ таких, что при согласованном изменении n и γ (напомним, рассматривается схема серий) конечен предел.

Необходимо $\lim\limits_{\gamma \to 0} (\lambda_i(\gamma)) = +\infty$, $i = 1,2$.

Положим

$$\lambda(\gamma) = \min\left(\lambda_1(\gamma); \lambda_2(\gamma)\right).$$

Г. Существует предел:

$$\lim_{\gamma \to 0} (\lambda_1(\gamma) / \lambda_2(\gamma)) \overset{def}{=} \lambda_0;\ 0 \leq \lambda_0 \leq +\infty. \tag{4}$$

То есть поведения процессов совершения атак и противоборства им асимптотически синхронизированы.

Д. При произвольном фиксированном значении переменной $x > 0$ соотношение (1) справедливо равномерно по всем $n \leq x\lambda(\gamma)$:

$$\lim_{\gamma \to 0}\{\max_{1 \leq n \leq x\lambda(\gamma)} \left| \overline{\varphi}_n(m(\gamma)z)(g_n(\gamma))^{-1} - \omega_n(z) \right| \} = 0. \tag{5}$$

Е. Равномерно по k и $n \leq x\lambda(\gamma)$, где a и b $(0 < a < b < +\infty)$ – произвольные числа, для любого $T \geq 1$ имеют место соотношения

$$\lim_{\gamma \to 0} \sum_{k=1}^{M} \sum_{j=1}^{T} \{Q_{i_j^{(k)}}(\gamma)\ \chi(i_j^{(k)} \leq x\lambda(\gamma))\} = 0; \tag{6}$$

$$\lim_{\gamma\to 0}\sum_{m\in N_k,\, m\le x\lambda(\gamma)} g_m(\gamma) \overset{def}{=} \mu_k(x), \qquad (7)$$

где $Q_n(\gamma) = g_n(\gamma) + q_n(\gamma)$ ($n \ge 1$), при $|N_k| < +\infty$ полагаем $Q_n(\gamma) = 0$ для $n > |N_k|$; $\chi(A)$ есть индикатор события A; множества N_k вводятся в [4] и представляют собой разбиение множества всех источников атак на группы однородных.

Требование выполнения соотношения (6) равносильно следующему условию: для любого $T \ge 1$ равномерно по k ($1 \le k \le M$) и $x\in(a, b)$, где a и b ($0 < a < b < \infty$) – любые числа, существуют пределы:

$$\lim_{\gamma\to 0}\left\{\sum_{k=1}^{n} Q_{i_j^{(k)}}(\gamma)\cdot\left(\sum_{m\epsilon N_{k,\, m\le x\lambda(\gamma)}} Q_{i_j^{(k)}}(\gamma)\right)^{-1}\right\} = 0. \qquad (8)$$

Асимптотическое поведение момента совершения первой успешной атаки

Как было указано выше, момент наступления первой успешной злоумышленной атаки в рамках введенной модели совпадает с моментом первого наступления редкого события, поэтому ниже основной результат формулируется на языке редких событий. Предварительно введем некоторые обозначения:

$$s_1(n)=\sum_{k=1}^{n} q_k(\gamma);\; s_2(n)=\sum_{k=1}^{n} T_k\sqrt{b^2-4ac};\; s_3(n)=\sum_{k=1}^{n}(q_k(\gamma))^2;$$

$$s_4(n)=\sum_{k=1}^{n}(T_k)^2;\; s_5(n)=\sum_{k=1}^{n} q_k T_k .$$

В работе [6] был выведен следующий результат.

Утверждение 1. Пусть выполнены условия А–Е. Тогда существует предел:

$$\lim_{\gamma\to 0} M\mathrm{e}^{-m(\gamma)z\tau_1} = \int_0^{\infty}\sigma_1(y)\, d_y(1-\exp\{-\sum_{k=1}^{M}\psi_k(z)\mu_k(y)-\sigma_1(y)\})\,. \qquad (9)$$

Ниже соотношение (9) и используется для получения основного результата работы.

Утверждение 2. Предположим, что выполнены следующие условия:

а) для любого $k \ge 1$существует $M\xi_k \overset{def}{=} T_k = T_k(\gamma)$, и для любых $\gamma > 0$ и $n > 0$ справедливы соотношения $(i = \overline{1,5})$: $s_i(n) = n^{\theta_i} L_i(n) G_i(\gamma)(1+\alpha_i(n, \gamma))$, где $\theta_i \ge 0$, $L_i(n)$ – медленно меняющиеся функции при $n \to \infty$, $\lim\limits_{\gamma\to 0} G_i(\gamma) = 0$, $\lim\limits_{\gamma\to 0}\lim\limits_{n\to\infty}\sup\limits_{|\tau|\le\gamma}|\alpha_i(n, \tau)| = 0$; и пусть $\lambda(\gamma)$ есть функция такая, что $\lim\limits_{\gamma\to 0} s_1(\lambda(\gamma)) = 1$;

б) для любого $x \ge 0$ равномерно по $n \ge 1$ существует предел

$$\lim_{\gamma\to 0}\{\frac{1}{T_n(\gamma)}\int_{xs_2(\lambda(\gamma))}^{\infty}(1-F_n(t))dt\} = 0; \qquad (10)$$

в) для любого $x \ge 0$ равномерно по $n \ge 1$ справедливо

$$\lim_{\gamma\to 0}\sup_{n\ge 1} q_n(\gamma) = 0.$$

Тогда существует предел ($z \ge 0$):

$$\lim_{\gamma\to 0} Me^{-z\frac{\tau}{M\tau}} = \int_0^{\infty} y^{\theta_1} d(1-\exp\{-\frac{z}{\Gamma(\theta_2/\theta_1+1)}y^{\theta_2}-y^{\theta_1}\}). \qquad (11)$$

При этом среднее время до первого отказа (до первой успешной злоумышленной атаки) равно

$$M\tau = \sum_{k=0}^{\infty} T_{k+1}\prod_{l=1}^{k-1}(1-q_l) \sim \Gamma(\frac{\theta_2}{\theta_1}+1)s_2(\lambda(\gamma)) \sim \Gamma(\frac{\theta_2}{\theta_1}+1)\,(\lambda(\gamma))^{\theta_2} L_2(\lambda(\gamma))G_2(\gamma) \qquad (12)$$

при $\gamma \to 0$ и $\lim\limits_{\gamma\to 0} M\tau = +\infty$. Здесь $\Gamma(x)$ – гамма-функция Эйлера.

В частности, если $\theta_1 = \theta_2 = \theta$, то предельное распределение в (11) представляет собой показательное распределение с параметром 1.

Докажем *утверждение 2*. Условие Б *утверждения 1* следует из условия в) *утверждения 2* (см. (10)).

Из определения функции $\lambda(\gamma)$ следует:

$$\lim_{\gamma\to 0} s_1(x\lambda(\gamma)) = \lim_{\gamma\to 0}\frac{s_1(x\lambda(\gamma))}{s_1(\lambda(\gamma))} = x^{\theta_1}\lim_{\gamma\to 0}\frac{L_1(x\lambda(\gamma))}{L_1(\lambda(\gamma))} = x^{\theta_1}. \qquad (13)$$

Пусть функция $m(\gamma)$ такова, что выполнено условие

$$\underline{\lim}_{\gamma\to 0}\{m(\gamma)^{-1}(s_2(\lambda(\gamma))^{-1}\} \ge 1. \qquad (14)$$

Отметим, что условие (14) допускает определенную многозначность выбора функции $m(\gamma)$, что приемлемо при выводе асимптотических соотношений.

Тогда для любого $u > 0$

$$\underline{\lim}_{\gamma\to 0}\{um(\gamma)^{-1}\} = \underline{\lim}_{\gamma\to 0}\{us_2(\lambda(\gamma))\}\,\underline{\lim}_{\gamma\to 0}\{m(\gamma)^{-1}(s_2(\lambda(\gamma)))^{-1}\} \ge$$

$$\ge \underline{\lim}_{\gamma\to 0}\{u\cdot s_2(\lambda(\gamma))\},$$

откуда, ввиду (10), следует: для любого $x > 0$ равномерно по $n \ge 1$

$$\lim_{\gamma\to 0}\{\frac{1}{T_n(\gamma)}\int\limits_{x(m(\gamma))^{-1}}^{\infty}(1-F_n(x))dx\}=0\,. \quad (15)$$

Полагая $\Phi_n(x,\gamma)=\dfrac{1}{T_n(\gamma)}\int\limits_0^{x(m(\gamma)^{-1})}(1-F_n(t))dt$, на основе (15) заключаем, что совокупность (по γ) вероятностных мер $\Phi_n(x, \gamma)$ при $\gamma \to 0$ равномерно по n сходится в собственном смысле к вероятностной мере, сосредоточенной в нуле. Отсюда, в силу замечания 2 [8, с. 317], следует, что для любого $z > 0$ равномерно по $n \ge 1$ существует предел

$$\lim_{\lambda\to 0}\frac{1-\varphi_n(m(\gamma)z)}{m(\gamma)T_n(\gamma)z}=\lim_{\lambda\to 0}\int\limits_0^{\infty}e^{-zu}d_u\{\frac{1}{T_n(\gamma)}\int\limits_0^{u(m(\gamma)^{-1})}(1-F_n(t))dt\}=\lim_{\lambda\to 0}\int\limits_0^{\infty}e^{-zu}d_u\{\Phi_n(\gamma,u)\}=1. \quad (16)$$

Соотношение (16) совпадает с соотношением (1), т. е. выполнено условие А с $g_n(\omega) = m(\gamma)T_n(\gamma)$, $\omega_n(z) = z$ $(n \ge 1)$. Далее, поскольку $z=\int\limits_0^{\infty}e^{-zu}d\chi(u)$, где $\chi(u)=1$ при $u \ge 0$ и $\chi(u)=0$ при $u < 0$, имеем:

$$\left|\frac{1-\varphi_n(m(\gamma)z)}{m(\gamma)T_n(\gamma)}-z\right|=\frac{1}{z}\left|\int\limits_0^{\infty}e^{-zu}d_u\{\chi(u)-\Phi_n(u,\gamma)\}\right|=\frac{1}{z}\int\limits_0^{\infty}e^{-zu}d_u\frac{1}{T_n(\gamma)}\int\limits_{u(m(\gamma))^{-1}}^{\infty}(1-F_n(t))dt\to 0 \quad (17)$$

при $\gamma \to 0$ равномерно по $n \ge 1$ ввиду условия (15). Следовательно, выполнено условие Д (см. (5)). Таким образом, при выполнении условия (13) имеют место условия А и Д.

Ввиду леммы 2 [4] выполняется соотношение

$$\lim_{n\to\infty,\, n\in N_k}\omega_n(z)=\psi_k(z)$$

с $M = 1$ и $\psi_k(z) = z$, т. к. $\omega_n(z) = z$ для всех $n \ge 1$.

Покажем, что условие (4) выполнено при $m(\gamma)=(M\tau)^{-1}\cdot\Gamma(\frac{\theta_2}{\theta_1}+1)$. Подсчитаем $M\tau$. Из (15) [6] имеем:

$$Me^{-z\tau}=a_1(z)=\sum_{k=1}^{\infty}(\varphi_k(z)-\varphi_k^+(z))\prod_{l=1}^{k-1}\varphi_l^+(z)=\sum_{k=1}^{\infty}(\varphi_k(z)\prod_{l=1}^{k-1}\varphi_l^+(z)-\prod_{l=1}^{k}\varphi_l^+(z))\,.$$

Отсюда после замены переменной $m = k - 1$ аналогично (16) [6] получаем:

$$a_1(z)=\varphi_1(z)+\sum_{k=2}^{\infty}(\varphi_k(z)\prod_{l=1}^{k-1}\varphi_l^+(z))-\sum_{m=2}^{\infty}\prod_{l=1}^{m-1}\varphi_l^+(z)=\varphi_1(z)+\sum_{k=2}^{\infty}(\varphi_k(z)-1)\prod_{l=1}^{k-1}\varphi_l^+(z)=$$
$$=\varphi_1(z)+\sum_{k=1}^{\infty}(\varphi_k(z)-1)\prod_{l=1}^{k-1}(\varphi_l(z)-\varphi_l^-(z))\,,$$

откуда следует:

$$M\tau=-a_1'(0)=-\varphi_1'(0)-\sum_{k=2}^{\infty}\varphi_k'(0)\prod_{l=1}^{k-1}(1-q_l)\,.$$

Так как $-\varphi'_k(0)=T_k$, то первая часть соотношений (12) *утверждения 2* доказана.

Из равенства (12) получаем:

$$M\tau=\int\limits_0^{\infty}\exp\{-\sum_{0\le l\le y}\ln(1-q_l)\}d_y\sum_{0\le l\le y}T_{l+1}=\int\limits_0^{\infty}\exp\{-\sum_{0\le l\le y\lambda(\gamma)}q_l(1+\Delta_l)\}d_y\sum_{0\le l\le y\lambda(\gamma)}T_{l+1},$$

где $|\Delta_l|\le\sup\limits_n q_n(\gamma)\to 0$ при $\gamma \to 0$ ввиду условия в) *утверждения 2*. Отсюда следует: при $\gamma \to 0$

$$M\tau=\int\limits_0^{\infty}\exp\{-s_1(y\lambda(\gamma))\}d_y s_2(y\lambda(\gamma))(1+o(1))\,.$$

Поскольку для $i = 1,2$ ввиду условия а) *утверждения 2* при фиксированном $\gamma > 0$ и $y \to \infty$ выполнено $L_i(y\lambda(\gamma))\sim L_i(y)$ и $\overline{\lim_{y\to\infty}}|\alpha_i(y\lambda(\gamma),\gamma)|<\infty$, то в силу условия а) *утверждения 2* имеем:

$$\lim_{y\to\infty}(e^{-s_1(y\lambda(\gamma))}s_2(y\lambda(\gamma)))=\lim_{y\to\infty}(\exp\{-(y\lambda(\gamma))^{\theta_1}L_1(y)G_1(\gamma)(1+\alpha_1(y\lambda(\gamma),\gamma))\}\times$$
$$\times(y\lambda(\gamma))^{\theta_2}L_2(y)G_2(\gamma)(1+\alpha_2(y\lambda(\gamma),\gamma)))=0\,.$$

Воспользовавшись последним соотношением в последнем интегральном соотношении для $M\tau$ и проведя интегрирование по частям, приходим к асимптотическому соотношению:

$$M\tau \sim \int_0^{\infty} s_2(y\lambda(\gamma))d_y(1-\exp\{-s_1(y\lambda(\gamma))\}).$$

На основе общего представления медленно меняющихся функций [9, с. 323], заключаем: при любом выбранном $\delta > 0$ можно выбрать постоянную величину $\gamma_1 > 0$ такую, что выполнено $\left|\varepsilon(\nu\lambda(\gamma))\right| < \delta$ при любом $\nu \geq 1$. Поэтому справедливо

$$\left|\frac{L_2(x\lambda(\gamma))}{L_2(\lambda(\gamma))}\right| = \left|\frac{c_2(x\lambda(\gamma))}{c_2(\lambda(\gamma))}\right| \cdot \exp\left\{\int_{\lambda(\gamma)}^{x\lambda(\gamma)} \frac{\varepsilon(u)}{u}du\right\} =$$

$$= \left|\frac{c_2(x\lambda(\gamma))}{c_2(\lambda(\gamma))}\right| \cdot \exp\left\{\int_1^x \frac{\varepsilon(t\lambda(\gamma))}{t}dt\right\} < \left|\frac{c_2(x\lambda(\gamma))}{c_2(\lambda(\gamma))}\right| \cdot \exp\left\{\int_1^x \frac{\delta}{t}dt\right\}.$$

Таким образом, при любых $\gamma > \gamma_1$ и $x \geq 1$ выполнено соотношение

$$\left|\frac{L_2(x\lambda(\gamma))}{L_2(\lambda(\gamma))}\right| < K_0 x^{\delta},$$

([9, с. 323]) $K_0 = \sup\limits_{x \geq 1}\left|\frac{c_2(x\lambda(\gamma))}{c_2(\lambda(\gamma))}\right| < \infty$. Так как $s_2(x\lambda(\gamma)) \leq s_2(\lambda(\gamma))$ при $x \leq 1$, то из последнего соотношения получаем:

$$\left|\frac{L_2(x\lambda(\gamma))}{L_2(\lambda(\gamma))}\right| < K_0(1+x)^{\delta}$$

для всех $x > 0$ и $\gamma > \gamma_1$.

Далее, совокупность вероятностных мер (по γ) $\{1-\exp\{-s_1(x\lambda(\gamma))\}\}$ при $\gamma \to 0$ сходится в собственном смысле к вероятностной мере $1-e^{-y^{\theta_1}}$ и, следовательно, в силу замечания 2 [8, с. 317], выводим: при $\gamma \to 0$ выполнено

$$M\tau \sim \int_0^{\infty} y^{\theta_2} d_y(1-e^{-y^{\theta_1}}) \cdot s_2(\lambda(\gamma)),$$

откуда следует асимптотическое соотношение (12).

Так как $-\int_0^{\infty} y^{\theta_2} de^{-y^{\theta_1}} = \Gamma(\frac{\theta_2}{\theta_1}+1)$, то из последнего соотношения получаем:

$$\lim_{\gamma \to 0}(s_2(\lambda(\gamma))\Gamma(\frac{\theta_2}{\theta_1}+1)(M\tau)^{-1}) = 1,$$

откуда выводим справедливость (13) с

$$m(\gamma) = (M\tau)^{-1}\Gamma\left(\frac{\theta_2}{\theta_1}+1\right).$$

Таким образом, условия А и Д имеют место при $m(\gamma) = (M\tau)^{-1}\Gamma\left(\frac{\theta_2}{\theta_1}+1\right)$.

Из условия а) *утверждения 2* выводим:

$$S_2(n,\gamma) \overset{def}{=} \sum_{k=1}^{n} g_k(\gamma) = m(\gamma)\sum_{k=1}^{n} T_k(\gamma) = m(\gamma)n^{\theta_2}L_2(n)G_2(\gamma)(1+\alpha_2(\gamma,n)) =$$

$$= \frac{n^{\theta_2}L_2(n)}{(\lambda(\gamma))^{\theta_2}L_2(\lambda(\gamma))}R_0(\gamma)(1+\alpha_2(\gamma,n)), \tag{18}$$

где $\lim\limits_{\gamma \to 0} R_0(\gamma) = 1$. Поскольку (см. (17)) $\lim\limits_{\gamma \to 0}\lambda(\gamma) = +\infty$, то из условия а) *утверждения 2* очевидно следует, что $\lim\limits_{\gamma \to 0}(\lambda(\gamma))^{\theta_2}L_2(\lambda(\gamma)) = +\infty$, и, в силу (18), получаем:

$$\lim_{\gamma \to 0} S_2(x\lambda(\gamma),\gamma) = x^{\theta_2}. \tag{19}$$

Выполнение условия В при $i = 1$ следует из условия а) *утверждения 2*, т. к. $s_1(n,\gamma) = S_1(n,\gamma)$. При $i = 2$ справедливость условия В следует из (18). Из условия а) *утверждения 2* следует $\lambda_1(\gamma) = \lambda(\gamma)$; из (18) также следует $\lambda_2(\gamma) = \lambda(\gamma)$. Отсюда вытекает $\lambda_2(\gamma)/\lambda_1(\gamma) = 1$, и, следовательно, выполнено условие Г.

Наконец, для проверки выполнения условия Е отметим, прежде всего, что число различных групп $M = 1$, т. к. $\omega_n(z) = z$ для всех $n \geq 1$. Поэтому условие (8) равносильно условию: для любого $T \geq 1$

$$\lim_{\gamma \to 0}\sum_{j=1}^{T} Q_j(\gamma)\chi(j \leq x\lambda(\gamma)) = 0,$$

которое вытекает из условий $\lim\limits_{\gamma\to 0} g_i(\gamma)=0$, $\lim\limits_{\gamma\to 0} q_i(\gamma)=0$ для всех $i \ge 1$.

Условие (7) равносильно условию $\lim\limits_{\gamma\to 0} \sum\limits_{m\le x\lambda(\gamma)} g_m(\gamma) = \mu_1(x)$.

Так как $\lim\limits_{\gamma\to 0} \sum\limits_{m\le x\lambda(\gamma)} g_m(\gamma) = S_2(x\lambda(\gamma))$, то последнее соотношение следует из (19). При этом $\mu_1(x) = x^{\theta_2}$.

Таким образом, мы доказали справедливость условий А–Е. При этом $M = 1$, $\sigma_1(x) = x^{\theta_1}$, $\mu_1(x) = x^{\theta_2}$, $\psi_1(z) = z$. Отсюда, в силу следствия 1 [6], следует соотношение:

$$\lim_{\gamma\to 0} Me^{-vm(\gamma)\tau} = \lim_{\gamma\to 0} M \exp\{-v\Gamma(\frac{\theta_2}{\theta_1}+1)\frac{\tau}{M\tau}\} = \int_0^\infty y^{\theta_1} d(1-\exp\{-vy^{\theta_2} - y^{\theta_1}\}).$$

Из последнего соотношения после замены переменной $v\Gamma(\frac{\theta_2}{\theta_1}+1) = z$ следует соотношение (11).

В частном случае $\theta_1 = \theta_2 = \theta$ получаем: $\Gamma(\frac{\theta_2}{\theta_1}+1) = 1$ и $\lim\limits_{\gamma\to 0} M \exp\{-z\frac{\tau}{M\tau}\} = \int\limits_0^\infty y^{\theta} d(1-\exp\{-zy^{\theta} - y^{\theta}\})$.

Отсюда после замены переменной $y^{\theta} = t$ выводим:

$$\lim_{\gamma\to 0} M \exp\{-z\frac{\tau}{M\tau}\} = \frac{1}{z+1}\int_0^\infty t d(1-\exp\{-t\}) = \frac{1}{z+1}.$$

Утверждение 2 доказано.

Таким образом, мы получили асимптотическое распределение (см. (11)) момента ближайшей атаки. Полученное распределение позволяет найти среднее время ожидания до момента ближайшей атаки, построить доверительные интервалы для разных уровней значимости, оценить вероятность злоумышленной атаки на конкретном временном интервале. Все перечисленные характеристики позволяют более адекватно реагировать на возможные атаки, предприняв, ввиду важности объекта, дополнительные усилия по повышению защиты информации на интервалах времени, где указанные характеристики указывают на повышенную вероятность злоумышленной атаки при степенном изменении интенсивности атак во времени.

Заключение

Полученный в работе результат показывает, что при весьма общих ограничениях на поведение исходных характеристик системы момент ближайшей злонамеренной атаки асимптотически сходится к некоторому из распределений из двухпараметрического класса, описываемого преобразованием Лапласа – Стилтьеса (11). Необходимо исследовать особенности поведения соответствующей функции распределения, что предполагается выполнить в последующих работах. Более того, при некоторых естественных дополнительных ограничениях, охватывающих практически большинство ситуаций применимости *утверждения 1*, предельное распределение оказывается экспоненциальным. Таким образом, при «разумных» ограничениях поведение момента ближайшей злонамеренной атаки при достаточно большом числе источников атак с высокой степенью точности подчиняется экспоненциальному закону. Отметим следующие важные особенности этого закона:

1) экспоненциальный закон обладает свойством «отсутствия памяти», т. е. время ожидания атаки, начиная с текущего момента, никак не зависит от времени ожидания этой атаки;

2) среднее значение экспоненциального закона и среднее отклонение совпадают, т. е. поток экспоненциально распределенных событий (атак) ведет себя крайне нестабильно, принимая то очень малые значения, то очень большие.

Указанные особенности потока злонамеренных атак порождают нередко «эффект неожиданности» в системе обеспечения ИБ и требуют принятия мер по поддержанию ее непрерывно в полной готовности.

Список источников

1. Гнеденко Д. Б., Соловьев А. Д. Одна общая модель резервирования с восстановлением // Изв. АН СССР. Техн. кибернетика. 1974. № 6. С. 113–119.

2. Гнеденко Д. Б., Соловьев А. Д. Асимптотическая оценка надежности сложных систем с быстрым восстановлением // Тр. III Всесоюз. школы-совещ. по теории массового обслуживания. М.: Изд-во МГУ, 1975. Т. 1. С. 185–197.

3. Соловьев А. Д. Асимптотическое поведение момента первого наступления редкого события в регенерирующем процессе // Изв. АН СССР. Техн. кибернетика. 1971. № 6. С. 79–90.

4. Попов Г. А., Попова Е. А., Бурмистрова О. В. Анализ входных условий в модели информационной безопасности, построенной на основе аппарата редких событий // Науч. вестн. НГТУ. 2019. Т. 3. С. 112–131.

5. Попов Г. А. Асимптотическое поведение момента первого наступления редкого события в неоднородном регенерирующем процессе // Депон. ВИНИТИ. № 2193-В00, 2000. 46 с.

6. Попов Г. А., Попов А. Г., Лаптев П. В. Формализация процесса изменения вероятности нарушения сервисов информационной безопасности на основе аппарата редких событий // Наука, образование, инновации: пути развития: материалы VIII Всерос. науч.-практ. конф. (Петропавловск-Камчатский, 23–25 мая 2017 г.). Петропавловск-Камчатский: Изд-во Камчат. ГТУ, 2017. С. 56–61.

7. Ткаченко А. В. Многоканальные системы обслуживания с неидентичными приборами: дис. … канд. физ.-мат. наук. М.: Изд-во МГУ им. М. В. Ломоносова, 2013. 108 с.

8. Шилов Г. Е. Математический анализ. Специальный курс. М.: ГИФМЛ, 1961. 436 с.

9. Феллер В. Введение в теорию вероятностей и ее приложения. М.: Мир, 1984. Т. 2. 738 с.

References

1. Gnedenko D. B., Solov'ev A. D. Odna obshchaya model' rezervirovaniya s vosstanovleniem [One common backup model with recovery]. *Izvestiya AN SSSR. Tekhnicheskaya kibernetika*, 1974, no. 6, pp. 113-119.

2. Gnedenko D. B., Solov'ev A. D. Asimptoticheskaya ocenka nadezhnosti slozhnyh sistem s bystrym vosstanovleniem [Asymptotic estimation of reliability of complex systems with fast recovery]. *Trudy III Vsesoyuznoj shkoly-soveshchaniya po teorii massovogo obsluzhivaniya.* Moscow, Izd-vo MGU, 1975. Vol. 1. P. 185-197.

3. Solov'ev A. D. Asimptoticheskoe povedenie momenta pervogo nastupleniya redkogo sobytiya v regeneriruyushchem processe [Asymptotic behavior of the moment of the first occurrence of a rare event in the regenerating process]. *Izvestiya AN SSSR. Tekhnicheskaya kibernetika*, 1971, no. 6, pp. 79-90.

4. Popov G. A., Popova E. A., Burmistrova O. V. Analiz vhodnyh uslovij v modeli informacionnoj bezopasnosti, postroennoj na osnove apparata redkih sobytij [Analysis of the input conditions in the information security model based on the apparatus of rare events]. *Nauchnyj vestnik NGTU*, 2019, vol. 3, pp. 112-131.

5. Popov G. A. *Asimptoticheskoe povedenie momenta pervogo nastupleniya redkogo sobytiya v neodnorodnom regeneriruyushchem processe* [Asymptotic behavior of the moment of the first occurrence of a rare event in an inhomogeneous regenerating process]. Deponirovano VINITI. N. 2193-V00, 2000. 46 p.

6. Popov G. A., Popov A. G., Laptev P. V. Formalizaciya processa izmeneniya veroyatnosti narusheniya servisov informacionnoj bezopasnosti na osnove apparata redkih sobytij [Formalization of the process of changing the probability of violation of information security services based on the apparatus of rare events]. *Nauka, obrazovanie, innovacii: puti razvitiya: materialy VIII Vserossijskoj nauchno-prakticheskoj konferencii (Petropavlovsk-Kamchatskij, 23–25 maya 2017 g.).* Petropavlovsk-Kamchatskij, Izd-vo Kamchat. GTU, 2017. Pp. 56-61.

7. Tkachenko A. V. *Mnogokanal'nye sistemy obsluzhivaniya s neidentichnymi priborami. Dissertaciya … kand. fiz.-mat. nauk* [Multi-channel service systems with non-identical devices. Dissertation ... cand. physico-mathematical sciences]. Moscow, Izd-vo MGU im. M. V. Lomonosova, 2013. 108 p.

8. Shilov G. E. *Matematicheskij analiz. Special'nyj kurs* [Mathematical analysis. Special course]. Moscow, GIFML, 1961. 436 p.

9. Feller V. *Vvedenie v teoriyu veroyatnostej i ee prilozheniya* [An introduction to probability theory and its applications]. Moscow, Mir Publ., 1984. Vol. 2. 738 p.

Статья поступила в редакцию 25.11.2024; одобрена после рецензирования 26.12.2024; принята к публикации 24.01.2025
The article was submitted 25.11.2024; approved after reviewing 26.12.2024; accepted for publication 24.01.2025

Информация об авторах / Information about the authors

Георгий Александрович Попов – доктор технических наук, профессор; профессор кафедры информационной безопасности; Астраханский государственный технический университет; pga_96@mail.ru

Georgiy A. Popov – Doctor of Technical Sciences, Professor; Professor of the Department of Information Security; Astrakhan State Technical University; pga_96@mail.ru

Надежда Валерьевна Давидюк – кандидат технических наук, доцент; заведующий кафедрой информационной безопасности; Астраханский государственный технический университет; davidyuknv@astu.org

Nadezhda V. Davidyuk – Candidate of Technical Sciences, Assistant Professor; Head of the Department of Information Security; Astrakhan State Technical University; davidyuknv@astu.org

Кирилл Дмитриевич Кузовлев – аспирант кафедры автоматизированных систем обработки информации и управления; Астраханский государственный технический университет; k.kuzovlev@astu.org

Kirill D. Kuzovlev – Postgraduate Student of the Department of Automated Information Processing and Control Systems; Astrakhan State Technical University; k.kuzovlev@astu.org

Шамиль Шавкетович Иксанов – доцент кафедры автоматизированных систем обработки информации и управления; Астраханский государственный технический университет; sh.iksanov@astu.org

Альберт Салманович Сафаралиев – студент, направление обучения «Информационная безопасность»; Астраханский государственный технический университет; albertsafaraliev@mail.ru

Shamil Sh. Iksanov – Assistant Professor of the Department of Automated Information Processing and Control Systems; Astrakhan State Technical University; sh.iksanov@astu.org

Albert S. Safaraliev – Student, direction of study “Information Security”; Astrakhan State Technical University; albertsafaraliev@mail.ru